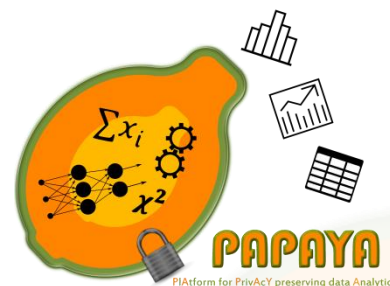


ANNOUNCEMENT LETTER




PAPAYA – Platform for PrivAcY preserving data Analytics

The PAPAYA project has officially started on May 1st, 2018 and is planned for three years. The project aims at enabling the execution of data analytics by third parties while keeping data confidential and hence complying with the new General Data Protection Regulation (GDPR).

Data analytics provide valuable insights and new opportunities to businesses who often resort to **third-party services or data processors** (such as clouds) to perform all these operations. Nevertheless, data analytics may jeopardize data **confidentiality** and data subjects' **privacy**, while companies and cloud providers must **comply with GDPR obligations**.

In this context, the **PAPAYA** project aims at enabling data processing and analytics on **encrypted and/or anonymized data**. This will ensure that data subjects' privacy is preserved while companies are still able to extract **valuable and meaningful information** from analyzed data.

Project ID:	786767
Start date:	May 1, 2018
Duration:	3 years
Total costs:	EUR 3 763 130
EC contribution:	EUR 2 949 417,50
Coordinator:	 EURECOM

Keywords:		
Data analytics	Privacy	Confidentiality
Machine learning	GDPR	Transparency
Platform	PETs	Dashboard
Usability	Audits	Control



PAPAYA's Objectives:

- ✓ Design efficient **privacy-preserving data analytics** techniques
- ✓ Explore **different settings** (single/multiple data owners, ...)
- ✓ Enable **risk management** and **user control** of data disclosure
- ✓ Design and develop an **integrated platform**
- ✓ Lead an **end-to-end analysis for 2 use cases**
- ✓ **Disseminate** and **exploit** the project outcomes

PAPAYA's Approach

• **Privacy-by-design**

PAPAYA will incorporate **privacy-enhancing technologies** (PETs) in data analytics tasks (which range from simple operations such as sum or average to more complex statistical tools such as machine learning algorithms), in the context of large amounts of data and multiple data sources.

• **Integrated platform**

The platform will offer ready-to-use privacy-preserving data analytics modules that can be used in interoperable manner.

• **Usability, Transparency and Auditability**

To facilitate user experience and enable data subjects and data controllers to exercise their rights over their data and control what is disclosed to third parties, the platform will provide the users with a dashboard featuring visualization and auditing components.



The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, through the PAPAYA project, under Grant Agreement No. 786767.



Visit! <http://www.papaya-project.eu/>



Follow! <https://twitter.com/ProjectPapaya>



Subscribe! <https://www.linkedin.com/company/papaya-project-eu-h2020/>

PAPAYA's Use Cases and Usage Scenarios

The project considers two use cases: UC1 dealing with **e-health data** and UC2 treating **web and mobile data**. Both use cases will cover several progressive scenarios.

UC1 – e-Health data

Thanks to the PAPAYA platform, a healthcare institution can **delegate** the processing of the tremendous amount of (sensitive) data collected by wearable devices and biomedical sensors to a **third-party processor** (e.g., a cloud). In a first scenario (Fig. 1.a), the healthcare institution (a **single data owner**) will encrypt the data and delegate the data analytics tasks to the cloud. The second scenario (Fig. 1.b) considers **several data owners** that collaborate to perform the analytics while keeping their **data confidential against each other**.

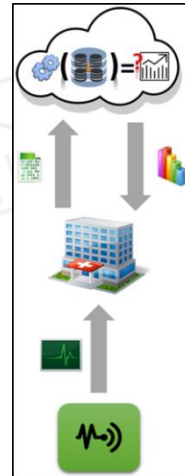


Fig. 1.a

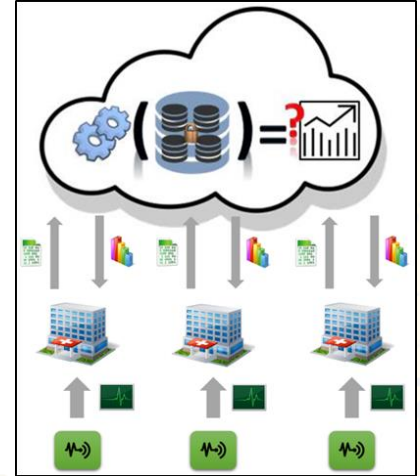


Fig. 1.b

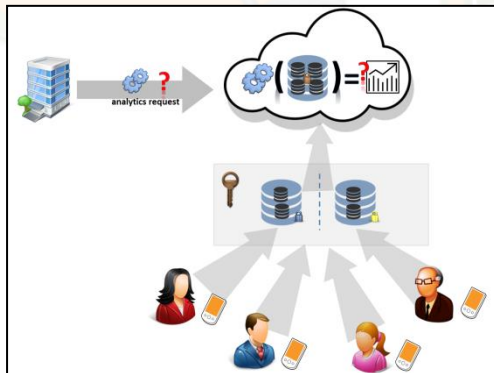


Fig. 2.a

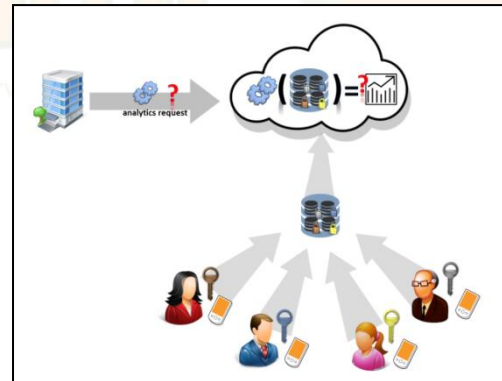


Fig. 2.b

UC2 – Web and mobile data

Web browsing and mobile data are useful for industries such as tourism to analyze tourists' flow. PAPAYA will be useful to extract such information in a privacy-preserving way. The first usage scenario (Fig. 2.a) considers a **single data owner** which **aggregates encrypted data** and allows a **third-party querier** to perform data analytics requests. In a second scenario (Fig. 2.b), **end-to-end privacy** will be ensured by **encrypting these data directly in users' mobile phones/devices**.

Consortium



Contact information

Project Coordinator

Melek Önen
EURECOM
Campus SophiaTech
450 route des Chappes
FR-06410 BIOT
melek.onen@eurecom.fr

Communication Leader

Sébastien Canard
Orange Labs
42 rue des Coutures
FR-14000 Caen
sebastien.canard@orange.com



The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, through the PAPAYA project, under Grant Agreement No. 786767.



Visit! <http://www.papaya-project.eu/>



Follow! <https://twitter.com/ProjectPapaya>



Subscribe! <https://www.linkedin.com/company/papaya-project-eu-h2020/>